[1] ГОСТ 34.003-90. Автоматизированные системы. Термины и определения. Утв. Постановлением Госкомитета СССР по управлению качеством продукции и стандартам от 27 декабря 1990 г. N 3399. М., 1990. С. 3.

[2] ГОСТ 34.201-89. Виды, комплектность и обозначение документов при создании автоматизированных систем. Утв. Постановлением Госкомитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 г. № 3468. М., 1990. С. 1.

[3] ГОСТ 34.601-90. Техническое задание. Требования к содержанию и оформлению. Утв. Постановлением Госкомитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 г. N 3469. М., С. 1.

[4] Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления: Утв. постановлением Минтруда России, 25 ноября 1994 г. № 72. – М., 1995. 116 с.

[5] Там же.

Е. П. Стрюкова

Уральский государственный университет

ПРОБЛЕМЫ ПРИМЕНЕНИЯ НА ПРАКТИКЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Применение на практике электронной цифровой подписи в Российской Федерации началось с середины 1990-х гг., преимущественно при заключении сделок. Участниками самостоятельно решались вопросы определения вида подписи и условий ее подлинности. Принятие в 2002 г. ФЗ «Об электронной цифровой подписи» (ЭЦП) должно было послужить стимулом к дальнейшему развитию применения ЭЦП на практике. Однако этого не произошло, т.к. главной проблемой ФЗ стала привязка нового вида подписи к технологии ее создания. Согласно закону подпись должна создаваться криптографическим способом. Общие алгоритмы формирования и проверки ЭЦП рассматриваются в ГОСТах Р34.10 – 2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»[1] и Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма»[2].

Операции формирования и проверки ЭЦП заложены в средство криптографической защиты информации (СКЗИ), которое должно иметь сертификат ФСБ.

К сожалению, сертифицированные СКЗИ, создаваемые различными российскими производителями, с помощью которых реализуются на прак-

тике единые российские криптографические стандарты, практически несовместимы между собой. Как правило, каждое из этих средств использует свои собственные идентификаторы алгоритмов, форматы представления их параметров и хранения ключевой информации. Соответственно сертификаты удостоверяющего центра (УЦ), построенного на базе одного СКЗИ, не смогут обслуживать криптосистемы, построенные на базе других СКЗИ, а подпись, сформированная одним СКЗИ, не может быть проверена другим СКЗИ.

Таким образом, алгоритмы, создающие ЭЦП, в одном УЦ не будут совместимы с алгоритмами другого УЦ. Это означает, что сертификат ЭЦП, выданный в одной системе инфраструктуры открытых ключей, не будет принят и проверен в другой системе. В то же время становится очевидным, что выданный для выполнения определенных действий сертификат ЭЦП должен иметь возможность подтверждения в любой системе, созданной для таких целей (например, для сдачи налоговых деклараций). Если процесс развития УЦ будет и дальше идти в том же направлении, то расхождения станут еще более существенными.

Нельзя не отметить, что предпринимаются попытки решить данную проблему так: 21 ноября 2003 г. ФГУП НТЦ "Атлас", ООО "Крипто-Про", ООО "Фактор-ТС", ЗАО МОПНИЭИ, ООО "Инфотекс" подписали соглашение об объединении усилий для осуществления совместных действий в целях достижения совместимости своих программных продуктов[3].

В 2006 г. была решена проблема совместимости СКЗИ на уровне сертификатов и форматов подписей. Ведущие производители средств СКЗИ выполнили работы, позволяющие проводить обмен информацией между системами, реализованными на разных средствах. Базовым стандартом «де-факто» стали разработки компании «Крипто-Про»[4]. Таким образом, в настоящее время, примерно в 21% российских УЦ используется по два программных решения СКЗИ. В таких УЦ используется решение криптопровайдера, которое было поставлено раньше, и наиболее популярная на данный момент «Крипто-Про». Это вызвано тем, что убирая старое СКЗИ и устанавливая новое, обеспечивающее совместимость сертификатов, придется требовать от клиентов установки новых СКЗИ, а это повлечет для клиентов материальные затраты. В результате для работы со старыми клиентами используется ранее существовавшее СКЗИ, а для работы с новыми – современные версии, обеспечивающие совместимость сертификатов различных криптопровайдеров.

Другая проблема заключается в том, что в рамках одного СКЗИ возможна разработка различных криптографических модулей для различных операционных систем и под разные системные требования. Криптографический модуль называется криптопровайдером или Cryptographic Service

Provider (CSP). Криптопровайдеры отличаются друг от друга по следующим параметрам:

1. состав функций (например, некоторые криптопровайдеры не выполняют шифрование данных, ограничиваясь созданием и проверкой цифровой подписи),

2. требования к оборудованию (специализированные криптопровайдеры могут требовать устройства для работы со смарт-картами для выполнения аутентификации пользователя).

Каждое программное средство разрабатывается под конкретную операционную систему. Наиболее популярным, конечно, является программное средство для операционной системы Windows корпорации Microsoft. Некоторые УЦ разрабатывают программные средства под Linux или Unix. Так, например, криптопровайдер для Windows, интегрируясь в эту операционную систему, сразу содержит библиотеку криптографических функций со стандартным интерфейсом. Он выполняет следующие функции:

- формирование/проверку ЭЦП,
- шифрование информации,
- хранение ключей всех типов.

Естественно, разработанный криптопровайдер для Windows не будет работать в Linux или Unix и наоборот.

Для создания юридически значимой ЭЦП необходимо использование только сертифицированных СКЗИ (следовательно, сертифицированных криптопровайдеров). На сегодняшний день в РФ сертифицированные криптопровайдеры – КриптоПроCSP, Signal-COM CSP (разработчик фирма КриптоПро), Домен-К (разработчик ИнфоТекс), «Верба-OW» (разработчик МОПНИЭИ), Di-POST (разработчик фирма «Фактор-ТС»), Signal-COM (разработчик компания «Сигнал-КОМ»), SmartCrypto (разработчик УЦ «АНКАД»), RSA (разработчик фирма Dekart).

Специалисты отмечают, что наиболее успешны УЦ, обслуживающие ЭЦП в собственных программных продуктах[5] (использующие собственную технологию создания ЭЦП).

В 2004 г. использовалось 9 технологий УЦ: КриптоПро, МОПНИЭИ, Microsoft CA, Infotecs, Keon, Baltimore UniCert, Фактор ТС, Инега, Сигнал Ком. В 2006 г. доминирующей становится технология УЦ КриптоПро (56%).

Все вышеперечисленные технологии создания ЭЦП используются как в государственном, так и коммерческом секторе.

Несмотря на то, что в министерствах и ведомствах можно все выстроить на единых принципах, эти учреждения строят автономные системы ЭЦП на технологически разнородных продуктах, используя к тому же различные организационные подходы. Так, в Пенсионном фонде РФ исполь-

зуется система «Контур-Эктерн», в Федеральной налоговой службе РФ – «Такском».

В коммерческом секторе ЭЦП активно используется в электронной торговле и электронном банкинге. Электронный банкинг более известен как система «клиент-банк» и «интернет-банк». Для аутентификации пользователя каждый банк использует свое программное обеспечение и несовместимые друг с другом форматы ЭЦП. Ни о какой совместимости говорить не приходится. Это вызывает справедливую критику со стороны клиентов, обслуживающихся в нескольких банках одновременно и вынужденных эксплуатировать множество программных пакетов и цифровых сертификатов ЭЦП, которые, по сути, предназначаются для решения однотипных задач.

Однако стоит отметить, что в решении этой проблемы, сделан важный шаг – подписанием в конце февраля 2003 г. Меморандума о создании «Ассоциации участников доверительного электронного документооборота». Его организаторами стали Ассоциация российских банков и Национальная ассоциация участников фондового рынка[6]. Главная задача этой Ассоциации – унификация использования соответствующего программного обеспечения в финансовой сфере.

В последние два-три года ЭЦП стала активно использоваться в сфере образования (преимущественно в дистанционном обучении студентов высших учебных заведений) и здравоохранении.

В процессе применения на практике ЭЦП возникла следующая проблема – распространение открытых ключей ЭЦП. Появляется необходимость создания электронного нотариуса или инфраструктуры открытых ключей (ИОК).

ИОК – это набор служб и сервисов для формирования, хранения, проверки, приостановления действия, обновления и отзыва цифрового сертификата. Применение ЭЦП подразумевает наличие развитой ИОК, поддерживающей, как минимум, функцию проверки целостности сертификата. Пользователи ИОК делятся на две категории: владельцы сертификатов и доверяющие стороны. Они используют некоторые сервисы и функции ИОК, чтобы получить сертификаты или проверить сертификаты других субъектов. Доверяющие стороны запрашивают и полагаются на информацию о статусе сертификатов и открытых ключах подписи своих партнеров по деловому общению.

В нашей стране вышеназванная инфраструктура только еще строится. И пока преждевременно говорить о том, что этот способ станет доминирующим в распространении открытых ключей.

В настоящее время рассматривается возможность использования электронного нотариуса (доверенная третья сторона). Суть создания такого нотариуса заключается в создании базы данных, содержащей сертификаты

ключей подписей. Нотариус должен будет подтверждать подлинность сертификата, его принадлежность и действенность.

Многие проблемы, возникающие в ходе применения ЭЦП на практике, в настоящее время решаются положительно. Главный принцип защиты ключевого материала – невозможность использования при попадании в чужие руки. Проще говоря, одним из основных условий гарантированного сохранения закрытого ключа в тайне (в соответствии с ФЗ) является сведение к минимуму риска (в идеале - исключение возможности) потери ключа, доступа к нему посторонних лиц и надежная защита ключа от копирования.

С другой стороны, важным аспектом в развитии применения на практике ЭЦП является сокращение рисков не только возможности подделки ЭЦП, но и в невозможности у автора электронной подписи отказа от совершенных им сделок в электронном виде. Собственно, для исключения такой возможности должна быть сформирована жесткая связь владельца сертификата ключей подписи с ЭЦП. Гораздо проще сформировать такую связь, если владельцу присваивается не только его личный сертификат, но и уникальный носитель закрытого ключа, никогда не покидающего защищенной памяти носителя. Однако для этого требуется реализация всех необходимых криптографических операций внутри носителя (токена, смарт-карты).

---

[1] ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Издательство стандартов, 2001.

[2] ГОСТ Р34.10-94 Информационные технологии. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе криптографического алгоритма. – М.: Издательство стандартов, 1994.

[3] ЭЦП — новый виток в развитии. [Электронный ресурс]/Режим доступа: http://eos.ru/eos/251390.// Электронные Офисные Системы [Электронный ресурс] — Электрон. дан — [Москва].:[2005]. — Режим доступа: http://eos.ru — Загл. с экрана. — Корректируется част

[4] Там же

[5] Анализ развития рынка удостоверяющих центров. Материалы IV международной научно-практической конференции «Сервисы удостоверяющих центров. Новые области применения PKI». [Электронный ресурс]/ Карпов А.Г. — Режим доступа: http://www.ank-pki.ru/conference/2006/presentation/Karpov A.G.pps// Центр технологических компетенций PKI. Закрытое Акционерное Общество АНК [Электронный ресурс]/. — Электрон. дан. — [Санкт-Петербург]: [200?]. — Режим доступа: http://www.ank-pki.ru. — Загл. с экрана. — Корректируется часто.

[6] Подписан меморандум о создании Ассоциации участников доверительного электронного документооборота [Электронный ресурс] - Режим доступа http://bankir.ru/news/newsline/20.03.2003/5268 //Ресурс о банках, для банкиров [Электронный ресурс], - Электрон. дан. – [Москва]: [2001-2008]. – Режим доступа: http://www.bankir.ru. – Загл. с экрана. – Корректируется часто.